CHAPTER

3

PLANNING NETWORK PROTOCOLS AND COMPATIBILITY

After reading this chapter and completing the exercises you will be able to:

- Explain basic network concepts, including network terms, types of networks, and network interface cards
- Explain the NDIS and ODI network driver specifications
- Explain the communications protocols used in Windows 2000 Server, including TCP/IP, NWLink, NetBEUI, DLC, and AppleTalk
- Plan network binding order, change the binding order, and bind and unbind protocols
- Plan how to implement protocols on different types of networks

Networking with Windows 2000 Server is about communication. Network communication takes place in many forms, including communicating with computers and printers, communicating with software applications, transporting e-mail, and providing Internet and intranet information exchange. The ability to communicate is made possible by using techniques that servers, workstations, and printers can agree upon. As you learned in the Chapter 1, Windows 2000 Server has a vast range of capabilities that enable networking on a small, medium, and large scale. Many of these capabilities are related to providing a common network language and enabling the translation of information between different kinds of networks and network operating systems.

When you set up a Windows 2000 Server, the first step is understanding the role of that server on the network and planning how to set up the server to meet that role. In this chapter, you will learn about the network communication services available through Windows 2000 Server and how to plan their optimal use in different situations. The chapter begins by providing you with networking basics that explain how communication occurs on a network. Next, you learn about network communications issues and about the communication languages, called protocols, that are used to address specific needs. You also learn how to plan network protocol implementations on different kinds of networks and how to improve network performance by setting the protocol binding order.

Basic Network Concepts

A computer or networking device communicates through a set of communications guidelines, in a way that is similar to using a language, but the language used by computers is in a binary format of zeros and ones that is sent through network communications cable. The communication languages of computers are called **protocols**. A protocol consists of guidelines for the following:

- How data is formatted into discrete units called packets and frames
- How packets and frames are transmitted across one or more networks
- How packets and frames are interpreted at the receiving end

Packets and **frames** are units of data transmitted from a sending computer to a receiving computer. These units might be compared to words in a language. In a language, people communicate by using words to compose sentences and paragraphs in order to convey a thought. The words by themselves do not convey the full thought until they are placed in the context of a sentence or paragraph. Like words, packets and frames usually do not convey their full meaning until the complete stream of information is received; and just as words must be properly placed in sentences and paragraphs, packets and frames must be received in the proper order to be understood.

Sometimes the terms *packet* and *frame* are used as if they have the same meaning. However, there is a difference between these terms, which is that a packet operates at a higher level of communication than does a frame. The higher level of communication associated with a packet enables it to contain routing information so that it can be forwarded from one network to another.

Packets and frames are divided into three general sections: a header, data, and a trailer. The header contains information that controls how the packet is transmitted, the data section contains the actual data that is transported, such as part of a Word file, and the footer is used to detect transmission errors. One of the most important functions of the header section is to house the addresses of the sender and receiver, called the source and destination addresses. Packets and frames use addressing, which is similar to the concept of addressing an envelope in the U.S. mail. Everyone is familiar with completing a surface mail envelope by providing the unique home or business address of the recipient and a return address. Network communications work in the same way, because the sender and receiver each have unique addresses and both addresses are included in the packet or frame so that there is a known destination and a way to return the communication in case the destination cannot be found or there is a delivery error. Also, in some protocols, the header and footer are used to indicate the beginning and end of a packet or frame. Figure 3-1 illustrates the basic packet or frame format.

Figure 3-1 Basic packet and frame format

Protocol, packet, and frame communication guidelines are established by standards organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), which represents over 140 countries. Two other standards organizations are the International Organization for Standardization (ISO), which has over 100 member countries, and the American National Standards Institute (ANSI), a United States organization that influences over 11,000 product standards and is an ISO member.

Types of Networks

The design of a network is its **topology**, which represents the overall layout of the network communications cable and the way in which packets and frames travel along the network. One or more network topologies are configured to form small, medium, and large-sized networks. A network that covers a relatively small distance, such as one that joins computers in the same office area or that links computers on different floors in a building is called a **local area network** (**LAN**). A LAN joins computers, printers, and other computer equipment within a limited service area and generally employs only one topology (see Figure 3-2).

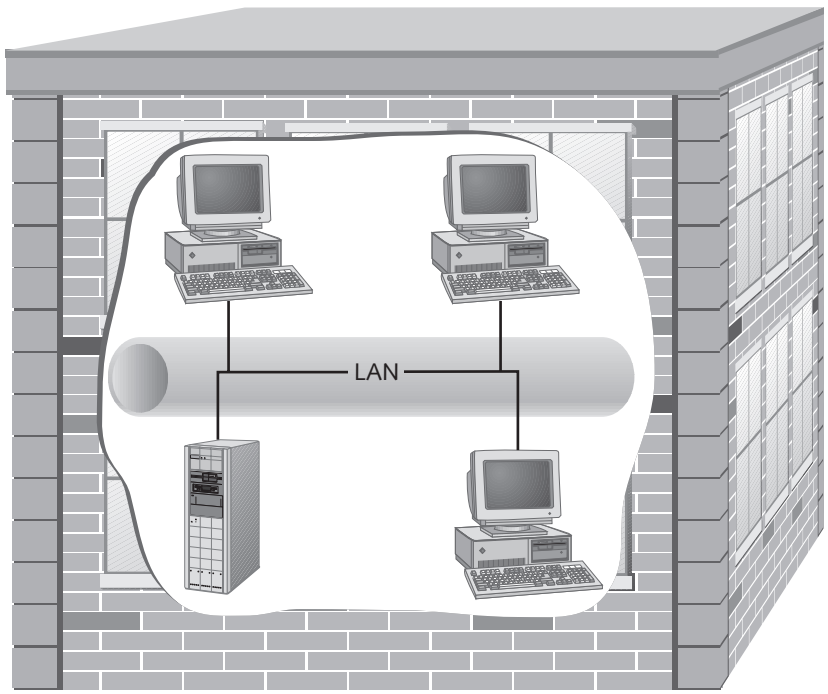

Figure 3-2 A LAN in a building

When multiple LANs are joined within a city or metropolitan region, the full network is called a **metropolitan area network** (**MAN**). A state university in one city is a MAN when it links several research centers and other facilities throughout the same city. In this example, there might be a veterinary lab on the edge of the city, an outreach branch in the center of the city, an observatory in another part of the city, a medical research facility in a hospital, and a main campus near the city center. A large business campus might have LANs used for administrative processing connected to LANs used for scientific research. Both of these also are examples of **enterprise networks** because they link a large array of resources for networked computers to use. The resources in an enterprise network may include mainframes, minicomputers, servers, printers, plotters, fax equipment, access to multiple networks, Internet access, intranets, and a vast range of software accessibility (see Figure 3-3).

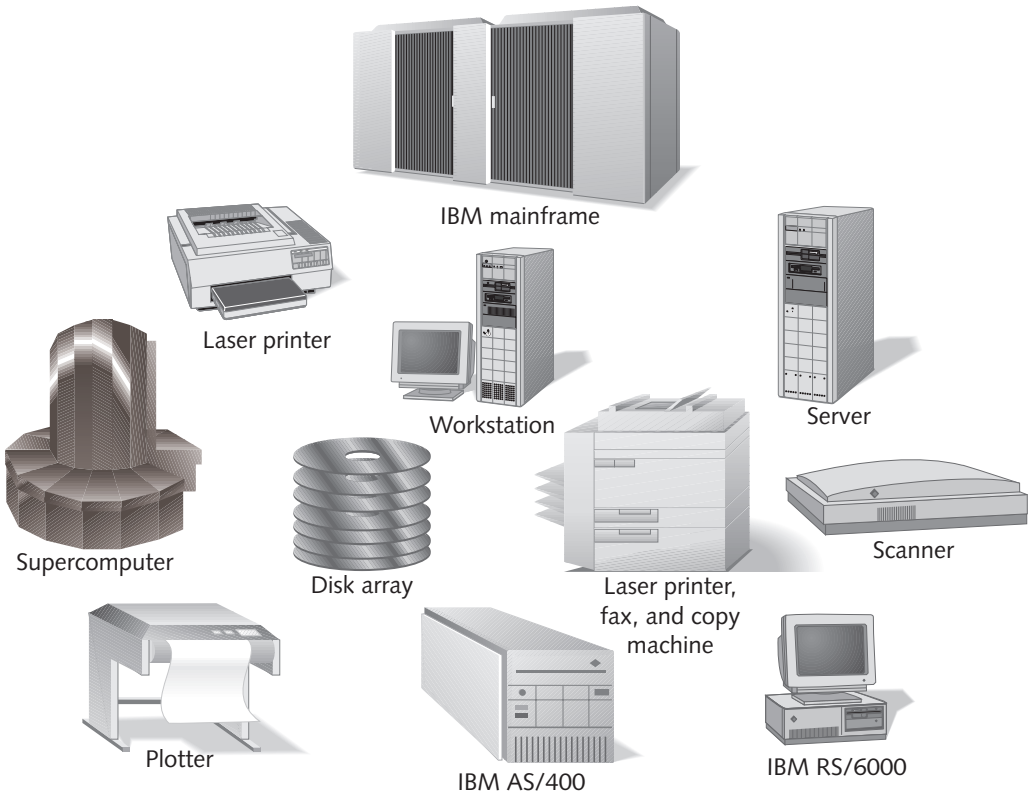

Figure 3-3 Resources in an enterprise network

A network that extends across cities, states, or continents is called a **wide area network** (**WAN**). For example, a multinational corporation with branch sites in New York, Toronto, London, and Stockholm can join the LANs at each site into a WAN that connects them all together. Another example of WAN communications is using the Internet to download new software from a company in Vancouver to your workstation in Los Angeles.

Network Interface Cards

The device used to connect a workstation, file server, or other network equipment to the communications cable is called its network interface card (NIC). The NIC contains a transmitter/receiver, or transceiver, for sending and receiving data signals on the cable. Each NIC comes with a set of software drivers to encode and decode the data so that it can be formatted to send on the cable and received data can be read by a workstation or server. NICs also have built-in memory chips to provide temporary storage while the data is waiting to be transmitted or to be sent to the computer's CPU for processing.

NICs are designed for the four main types of network communication media: coaxial cable, twisted-pair cable, fiber-optic cable, and wireless communications (such as radio waves). Some NICs come with adapters for both coaxial and twisted-pair cable. Figure 3-4 shows a NIC with the capability to connect to twisted-pair or coax cable (although you should not connect both at the same time). Many vendors sell computers with the NIC already installed, for college and business customers. (Try Hands-on Project 3-1 to experiment with a NIC.)

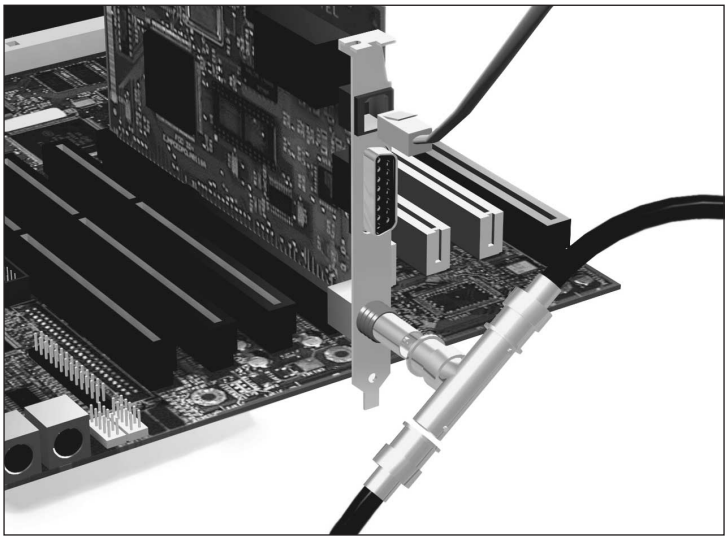

Figure 3-4 Connecting cable to a NIC

Each workstation and server has a unique address associated with its NIC, which is called the **physical address** or **device address** and is burned into a Programmable Read-only Memory chip (PROM) in the NIC. (Try Hands-on Projects 3-2 and 3-3 to view the physical address of a NIC.) To prevent confusion on the network, it is important that no two network cards have the same address. If this should happen and both NICs are active, network communications become unreliable, because it is difficult for the network to determine if packets are being sent or received by a single, distinguishable node.

Network administrators often refer to the physical address as the media access control (MAC) address, which is a more technical reference to the **media access control sublayer** of the

data-link layer (Layer 2) in the Open Systems Interconnection (OSI) model. The OSI model was developed for network communications by the ISO and ANSI. The MAC sublayer examines physical address information in frames and controls the way devices share communication on a network.

Network Driver Specifications

Windows 2000 network communication is accomplished through three elements:

- A network driver specification built into Windows 2000
- The NIC
- A NIC software driver that interfaces the NIC with Windows 2000

The network driver specification might be thought of as a door into a portion of the operating system, providing a means to link the computer to the network. In a sense, the network driver specification is a set of rules that represents a lock, and the NIC driver provides a key to open the lock so that the operating system can communicate on the network through the NIC. The network driver specification includes guidelines for **Ethernet** or **token ring** communications, and guidelines for specific communication protocols used within Ethernet and token ring. It also provides a way to encapsulate and transport multiple protocols on the same network. Each NIC manufacturer provides a driver for their NIC that conforms to the network driver specification used by an operating system, such as Windows 2000 Server. Microsoft also provides NIC drivers on the Windows 2000 Server CD-ROM.

Windows 2000 Server uses the Network Driver Interface Specification (NDIS). Another specification, which is used on Novell NetWare networks, is the Open DataLink Interface (ODI).

NDIS

Created by Microsoft and 3COM, the **Network Driver Interface Specification** (**NDIS**) is a network software driver specification that enables Microsoft network protocols to communicate with a NIC. When you bind a protocol to a NIC, this is accomplished through the NDIS driver. **Network binding** is a process that identifies a computer's NIC with one or more network protocols to achieve optimum communications with network services. For Microsoft operating systems, each protocol that is installed is bound to the NIC during the installation process (Figure 3-5).

NDIS can bind one or more protocols to a single NIC, allowing each protocol to send information on the same network. For example, you may have one process sending information using the TCP/IP protocol while another process is sending information using the NWLink (IPX/SPX) protocol to communicate with a Novell NetWare server (you learn about these protocols later in this chapter).

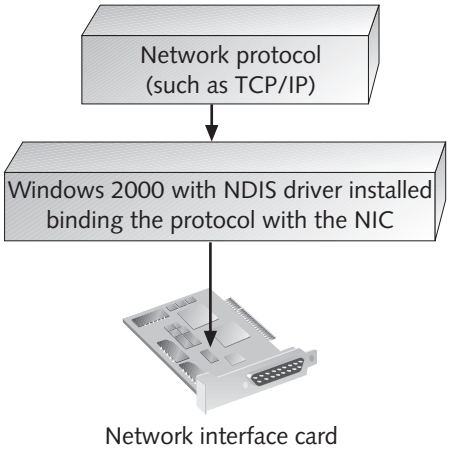

Figure 3-5 Binding a protocol to a NIC

ODI

Another driver that is used to transport multiple protocols is the **Open Datalink Interface** (**ODI**) driver. This driver is used on Novell NetWare networks to support communications with NetWare file servers, mainframes and minicomputers, and the Internet, similarly to NDIS.

ODI communications can be used on older Microsoft networks, such as networks that use Windows NT 3.5x and 4.0 Server, but this is not advised. The best preparation for upgrading to Windows 2000 Server is to convert Windows NT 3.5x and 4.0 Server versions to use the 32-bit NDIS driver for network communications, if they are not already using NDIS.

COMMUNICATIONS PROTOCOLS

Windows 2000 Server supports several communications protocols to provide network services over LANs and WANs: TCP/IP, NWLink (IPX/SPX), NetBIOS/NetBEUI, DLC, and AppleTalk. Any or all of these protocols can be bound to a Windows 2000 server's NIC via NDIS. The communications protocols are summarized in Table 3-1 and described in detail in the following sections.

Table 3-1 Microsoft-supported Communications Protocols

Protocol	Function
TCP/IP (Transmission Control Protocol/Internet Protocol)	Software drivers for TCP/IP communications with servers, workstations, mainframes, UNIX computers, and Internet and intranet servers
NWLink (NetWare Link)	Microsoft developed drivers for communications with Novell NetWare networks
NetBIOS (Network Basic Input/Output System)	A link to programs that use the NetBIOS interface
NetBEUI (NetBIOS Extended User Interface)	Software drivers for a data transport protocol used on small Microsoft-based networks
DLC (Data Link Control protocol)	Software drivers for communication with IBM mainframe and minicomputers and with specific peripherals such as some types of printers
AppleTalk	Software drivers for communication with Apple Macintosh computers

TCP/IP

One important difference between Windows 2000 Server and earlier versions of Windows NT Server is that TCP/IP takes center stage in Windows 2000 as the protocol of choice. Small and large networks increasingly need TCP/IP for Internet, World Wide Web (Web), and intranet connectivity. Also, as more LANs grow into enterprise networks and connect to WANs, TCP/IP is needed because it is ideal for communications that go over dissimilar networks. Further, many networks require connectivity to a host computer, such as a mainframe running IBM's Multiple Virtual Storage (MVS) operating system or a minicomputer with UNIX. The protocol for all of these jobs is **Transmission Control Protocol/Internet Protocol** (**TCP/IP**). TCP/IP is used around the globe for reliable network communications. TCP/IP is many protocols wrapped into one, all working together to establish the most error-free communications possible. The TCP portion was originally developed to ensure reliable connections on government, military, and educational networks. TCP provides for reliable end-to-end delivery of data by controlling data flow. Nodes agree upon a "window" for data transmission that includes the number of bytes that will be sent. The transmission window is constantly adjusted to account for existing network traffic. TCP/IP monitors for requests to start a communications session, establishes sessions with other TCP nodes, handles transmitting and receiving data, and closes transmission sessions when they are finished. TCP is also considered a **connection-oriented communication** because it ensures that packets are delivered, that they are delivered in the right sequence, and that their contents are accurate.

Some applications use the **User Datagram Protocol** (**UDP**) with IP instead of using TCP. These are typically applications in which the reliability of the communication is not a major concern, such as for information used to boot diskless workstations over a network. UDP is a **connectionless communication** because it does not provide checking to make sure that a connection is reliable and that data is sent accurately. The advantage of UDP is that it has less overhead than TCP.

The IP portion of the TCP/IP protocol provides network addressing to ensure that data packets and frames quickly reach the correct destination. It uses a system of addressing that consists of four numbers separated by periods, such as 129.77.15.182. IP provides for routing data over different networks, so that data sent from one network only goes to the appropriate destination network instead of to all networks that are linked together. IP also handles fragmenting packets, because the packet sizes may vary from one network to another. IP is connectionless communication because it relies on TCP to provide connection-oriented communications.

The combination TCP/IP protocol is particularly well suited for medium and large networks, but it is important on any enterprise network or on a LAN that connects to a WAN.

Before upgrading Windows NT 3.5x and 4.0 servers to Windows 2000, Microsoft recommends that you convert them and their client workstations to TCP/IP, if it is not already implemented (you can practice converting Windows NT Server 4.0 to TCP/IP in Hands-on Project 3-4). Also, work to eliminate the use of any other protocols, such as NetBEUI or NWLink, unless these are required to support connectivity to older servers and printers, such as to NetWare version 4 or earlier servers.

IP Addressing

The IP address format is called the **dotted decimal notation** address. It is 32 bits long and contains four fields, consisting of decimal values representing 8-bit binary octets. An IP address in binary octet format looks like this: 10000001.00000101.00001010.1100100, which converts to 129.5.10.100 in decimal format. Part of the address is the network identifier (NET_ID), and another part is the host identifier (HOST_ID), the way the parts are designated depends on the size of the LAN, how the LAN is divided into smaller networks, and if the packet or frame is unicast or multicast. A unicast is a transmission in which one packet is sent from a server to each client that requests a file or application, a video presentation for example. Thus, if five clients request the video presentation, the server sends five packets per each transmission to the five clients. In the same example, a multicast means that the server is able to treat all five clients as a group and send one packet per transmission that reaches all five clients (see Figure 3-6). Multicasts can be used to significantly reduce network traffic when transmitting multimedia applications.

In a unicast on a typical medium-sized LAN of up to 65,536 connections, the first two octets are normally the network ID, and the last two are the host ID. In a multicast transmission on the same network the four octets are used to specify a group of nodes to receive the multicast, which consists of those nodes that are multicast subscription members.

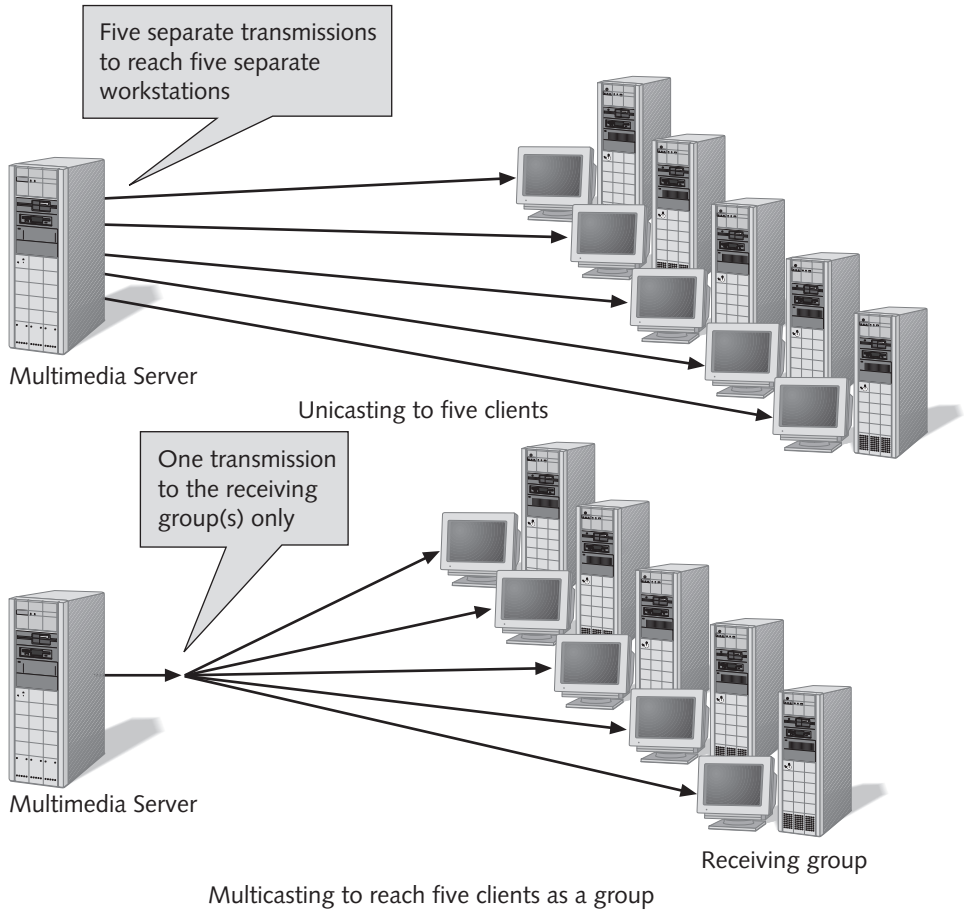

Figure 3-6 Unicasting compared to multicasting

Another special-purpose form of addressing is the **subnet mask**. A subnet mask is used for two purposes: to show the class of addressing used, and to divide a network into subnetworks to control network traffic. In the first instance, the subnet mask enables an application to determine which part of the address is for the network ID and which is for the host ID. For example, a subnet mask for a Class A network is all binary 1s in the first octet and all binary 0s in remaining octets: 11111111.00000000.00000000.00000000 (255.0.0.0 in decimal). Figure 3-7 shows the IP address and subnet mask setup dialog box in Windows 2000.

To divide the network into subnetworks, the subnet mask consists of a subnet ID within the network and host IDs, which are determined by the network administrator. For example, the entire third octet in a Class B address could be designated to indicate the subnet ID, which would be an octet of 11111111.11111111.11111111.00000000 (255.255.255.0). Another option would be to designate only the first 5 bits in the third octet as the subnet ID and the last 3 bits (and last octet as well) for the host ID, which would be 11111111.11111111.11111000.00000000 (255.255.248.0).

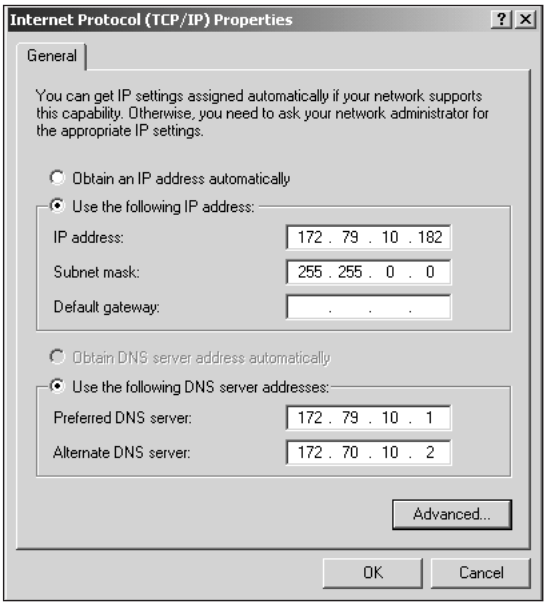

Figure 3-7 IP address and subnet mask setup

Many server administrators use TCP/IP because the ability to create subnets provides important versatility in controlling network congestion and in setting up security so that only authorized users can reach specific parts of a network or specific intranets.

Static and Dynamic Addressing

Each server and workstation needs a unique IP address, either specified at the computer or obtained from a server that assigns temporary IP addresses. Before setting up TCP/IP, you need to make some decisions about how to set up IP addressing on the network. The options are to use what Microsoft calls static addressing or dynamic addressing. **Static addressing** involves assigning a dotted decimal address that is each workstation's permanent, unique IP address. This method is used on many networks, large and small, when the network administrator wants direct control over the assigned addresses. Direct control may be necessary when network management software is used to track all network nodes and the software depends on each node having a permanent, known IP address. Permanent addresses give consistency to monitoring network statistics and to keeping historical network performance information. The disadvantage is that IP address administration can be a laborious task on a large network. Most network administrators have an IP database to keep track of currently assigned addresses and unused addresses to assign, as new people are connected to the network.

Dynamic addressing automatically assigns an IP address to a computer each time it is logged on. An IP address is leased to a particular computer for a defined period of time. This addressing method uses the **Dynamic Host Configuration Protocol** (**DHCP**), which is supported by Windows 2000 Server for dynamic addressing. The protocol is used to enable

a Windows 2000 server with DHCP services set up to detect the presence of a new workstation and assign an IP address to that workstation. On your network, this would require you to load DHCP services onto a Microsoft 2000 server and configure it to be a DHCP server. It would still act as a regular server for other activities, but with the added ability to automatically assign IP addresses to workstations. A Windows 2000 DHCP server leases IP addresses for a specified period of time, which might be one week, one month, one year, or a permanent lease. When the lease is up, the IP address is returned to a pool of available IP addresses maintained by the server. On Windows 2000 servers that provide Internet communication, when one is configured as a DHCP server, **Windows Internet Naming Service** (**WINS**) is also installed so that the Windows 2000 Server is both a DHCP and a WINS server. A WINS server is able to translate a workstation name to an IP address for Internet communication, for example translating the workstation name, Palmer, to its IP address, such as 129.77.15.182.

When you use DHCP, plan to apply it to client workstations and not to servers, or to make each server's IP address permanent. It is important for server IP addresses to always remain the same so there is no doubt about how to access a server. For example, consider how hard a Web server would be to find on the Internet if its IP address changed periodically.

TCP/IP Advantages and Disadvantages

There are several advantages that TCP/IP offers:

- It is very well suited for medium to large networks, for enterprise networks, and for any network that has Internet connectivity or uses intranets.
- It is designed for routing and has a high degree of reliability.
- It is used worldwide for connecting to the Internet and for using intranets.
- It is key to Microsoft's strategy to accomplish a lower Total Cost of Ownership (TCO), and to many of the new features of Windows 2000 Server such as application services management, Zero Administration for Windows (ZAW), and Distributed Network Architecture (DNA; see Chapter 1).
- It is compatible with standard tools for analyzing network performance.
- It enables the use of DHCP and WINS through a Microsoft 2000 Server.
- It provides the ability for diverse networks and network operating systems to communicate via LANs and WANs, and scales easily from small to large networks.
- It is compatible with Microsoft Windows Sockets, which is used by software applications, for example for client/server and telecommunications connectivity.

Windows Sockets (WinSock) interfaces software applications that use "sockets" with network protocols such as TCP/IP and IPX. Created by the University of California at Berkeley, WinSock is an open specification in Windows operating systems for different network protocol functions that use different addressing methods (sockets). Windows 2000 DHCP Server is one example of an application that uses WinSock.

TCP/IP does have some disadvantages as well:

- It is more difficult to set up and maintain than other protocols.
- It is somewhat slower than IPX/SPX and NetBEUI on networks with light to medium traffic. (However, it may be faster on heavy volume networks, where there is a high frequency of routing frames.)

One situation in which you would use TCP/IP would be on a large enterprise network, such as on a college or business campus, where there is extensive use of routers and connectivity to mainframe or UNIX computers. A **router** is a device that connects networks, is able to read IP addresses, and can route packets to designated networks, because it reads routing information in packets (OSI Layer 3) and keeps tables of information about the fastest route from one network to another (see Figure 3-8). You also would use it in a smaller network situation, in which 100–200 Windows-based workstations access intranet or Internet services through a Windows 2000 server offering Web services, using Microsoft's Internet Information Server.

Protocols in the TCP/IP Suite

Complementing the main TCP/IP protocols are several application protocols and services that help make up the TCP/IP "protocol suite":

- **Telnet**: This is an application protocol within TCP/IP that provides support for terminal emulation, for example for an IBM 3270 terminal or a DEC VT220 terminal. Telnet enables a user to connect to a host computer so that the host responds as though it were connected to a terminal.
- **File Transfer Protocol** (**FTP**): This is a protocol that enables the transfer of data from one remote device to another, using the TCP and Telnet protocols. Through FTP, a user in England can use the Internet to log on to a host computer in California and download one or more data files from the host.
- **Simple Mail Transfer Protocol** (**SMTP**): This protocol is designed for the exchange of electronic mail between networked systems. Windows 2000, UNIX, NetWare and other computer operating systems can exchange messages if they have TCP/IP accompanied by SMTP. SMTP is particularly useful for electronic mail that goes over the Internet.

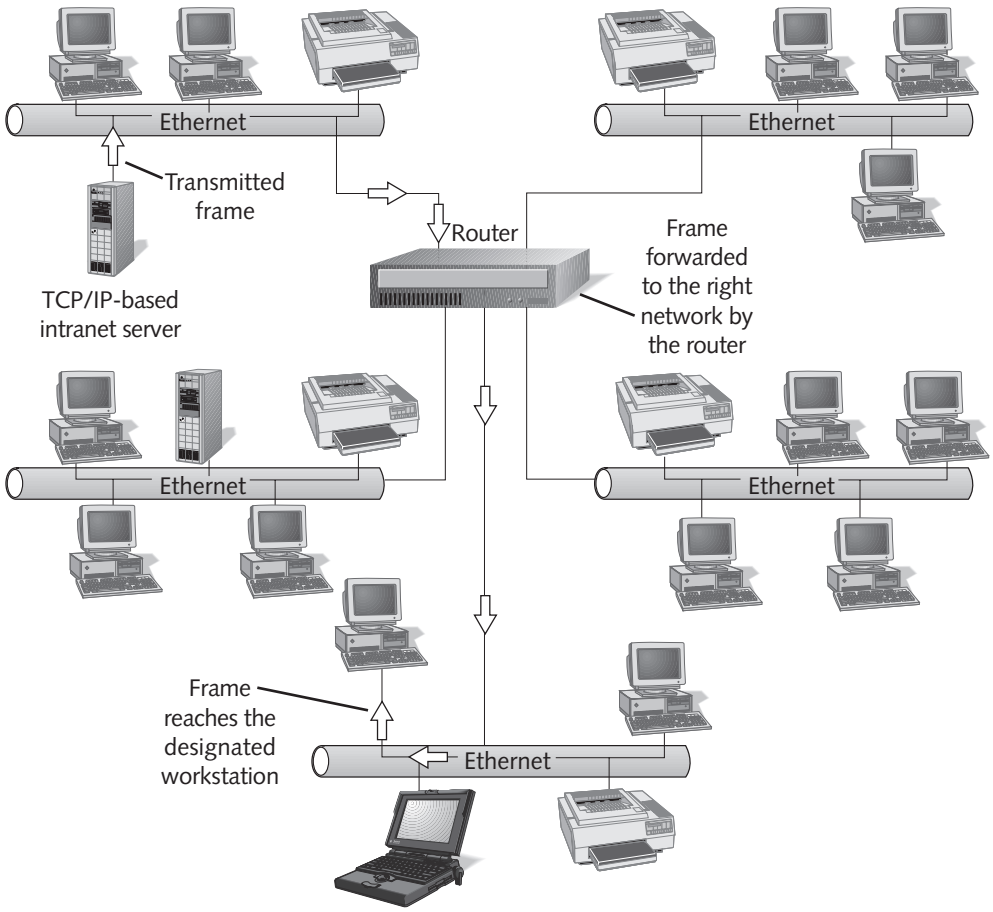

Figure 3-8 Router forwarding packets to a designated network

- **Domain Name Service** (**DNS**): This service is particularly important to Windows 2000 Server when the Active Directory is installed. DNS is used to translate domain and computer names, such as *microsoft.com*, to an IP address (and vice versa). The DNS software runs on one computer that acts as a network zserver for the address translations. The process of translating names to addresses is called resolution, a process you have already used if you access the Internet. Windows 2000 Server can be set up to act as a DNS server on a network. Often there are at least two DNS servers set up on a network, one to act as the primary server and one to act as a secondary, or backup, server in case the primary DNS server cannot be reached. Windows 2000 Server offers dynamic DNS services, which means that a new network client can discover the DNS server and add its own DNS entry without you manually entering it. Plan to implement dynamic DNS services to reduce your administrative tasks.
- **Address Resolution Protocol** (**ARP**): This protocol enables a sending node to obtain the IP and MAC addresses of the intended recipient before packets are

sent. ARP is used by network management software and by DHCP servers to help determine the actual location of a client workstation.

- **Simple Network Management Protocol** (**SNMP**): This protocol is used by network managers and network management software to gather statistics on network performance and to locate network problems. SNMP's ability to quickly help identify server and network problems is one important reason why TCP/IP is popularly used on networks. It is also critical to Windows 2000 servers that use network monitoring software, such as Microsoft's Network Monitor.
- **Internet Group Management Protocol** (**IGMP**): This protocol is used when an application employs multicasting. Both the server and client workstations must be configured for multicast operations, and so are configured to use IGMP. The routers in between the server and workstations also are configured for multicasts. One important function of IGMP is to keep routers informed of which workstations belong to which multicast groups to make sure that multicast packets reach the right workstations.
- **Internet Control Message Protocol** (**ICMP**): This protocol is used for network error reporting, particularly through routing devices. ICMP enables network administrators to locate and determine network problems. For example, ICMP enables a network administrator to poll a device to determine if it is connected to the network (try Hands-on Project 3-5).
- **Routing Information Protocol** (**RIP**): This protocol is used by routing devices to share network information with one another. For example, it is used by routers to share tables in which they keep information about the location of specific computers on the network (stored in a routing table). RIP also enables routing devices to determine the shortest path from one network location to another, and share that information with other routing devices.
- **Open Shortest Path First** (**OSPF**) **protocol**: Designed to be more efficient than RIP, OSPF is a routing protocol that shares routing table information and that can set up routes to match the type of transmission, such as data or video.
- **Hypertext Transfer Protocol** (**HTTP**): This protocol enables the transport of Hypertext Markup Language (HTML) documents over the Internet. These are the documents that you read through an HTTP-compliant browser, such as Microsoft Internet Explorer and Netscape Communicator, providing access to text and embedded audio, video, and graphics files.
- **Resource Reservation Protocol** (**RSVP**): This protocol enables network resources to be reserved for specific kinds of high-demand uses, such as for multimedia applications that combine audio and video in a news clip, movie, or instructional application. RSVP enables an application to reserve the resources it needs, such as network paths with higher speeds. By implementing RSVP, network-hungry multimedia applications can coexist with less demanding simple data applications, but they can be given a higher delivery priority because they are more time-sensitive.

- **Quality of Service** (**QoS**): Often used with RSVP, this service consists of network transmission techniques that are used to help guarantee the transmission quality, throughput, and reliability of a network system. The overall goals of QoS are to ensure that the proper network resources are assigned to specific applications and to reduce the likelihood that valuable network resources are underutilized. QoS is used for multimedia, telephony, and mission-critical applications to help guarantee they have appropriate resources, such as time-sensitive communications. In Windows 2000 Server, the Active Directory verifies that an application or user has authority to use QoS and to assign a high priority for a transmission. The QoS capabilities that can be accessed in Windows 2000 Server via TCP/IP with RSVP are:
  - Admission Control Service (ACS), which enables you to reserve network resources through policies that you establish in the Windows 2000 Active Directory
  - Differentiated Quality of Service, which provides utilities to allocate resources to applications, such as allocating high-speed network routes to multimedia or client/server applications
  - Prioritized LANs (based on the IEEE 802.1p standard) to give specific applications, such as audio e-mail high priority, and other applications, games for example, lower priority

Table 3-2 provides a summary of the applications and protocols in the TCP/IP suite that are discussed in this chapter and supported by Windows 2000 Server.

Table 3-2 Protocols and Applications in the TCP/IP Suite

Protocol or Application	Function
TCP	A connection-oriented protocol that is used with IP for reliable end-to-end communications
UDP	Used with IP as an alternative to TCP in situations requiring low overhead and in which connectionless communications are appropriate
IP	Used with TCP or UDP, a connectionless protocol that handles addressing and routing
Telnet	Provides terminal emulation
File Transfer Protocol (FTP)	Used to transfer files
Simple Mail Transfer Protocol (SMTP)	Provides electronic mail services
Domain Name Service (DNS)	Resolves computer names to IP addresses, and IP addresses to computer names
Address Resolution Protocol (ARP)	Enables the sending node to determine the MAC or physical address of another node
Simple Network Management Protocol (SNMP)	Enables computers and network devices to gather network performance information so that a network administrator can analyze performance and locate problem areas

Table 3-2 Protocols and Applications in the TCP/IP Suite (continued)

Protocol or Application	Function
Internet Group Management Protocol (IGMP)	Enables multicast packets to reach their recipients, and routers to determine which workstations belong to a multicast group
Internet Control Message Protocol (ICMP)	Used for network error reporting, particularly via routing devices
Routing Information Protocol (RIP)	Used by routing devices to communicate the contents of routing tables with one another
Open Shortest Path First (OSPF)	Used by routing devices to share routing table information and to evaluate network paths to match a type of transmission to the appropriate path
Hypertext Transfer Protocol (HTTP)	Used to transport HTML documents over the Internet or via an intranet
Resource Reservation Protocol (RSVP)	Used to enable a network application to reserve the resources it needs, such as bandwidth, service class, and priority
Quality of Service (QoS)	Provides mechanisms to measure and allocate network resources on the basis of transmission speed, quality, priority, and reliability.

NWLink and IPX/SPX

Some Novell NetWare servers use a connectionless protocol called the **Internet Packet Exchange** (**IPX**) protocol. IPX is used mainly on NetWare version 4.x and earlier servers. NetWare version 5.x servers typically use TCP/IP instead of IPX.

IPX, like TCP/IP, has routing capabilities, so data is transported over multiple networks in an enterprise. Along with IPX, Novell implements a companion protocol called **Sequence Packet Exchange** (**SPX**). SPX enables the exchange of application-specific data with greater reliability than IPX because it is a connection-oriented communication, whereas IPX is connectionless. One use of SPX is for the exchange of database data on the network. Novell's remote console utility and print services also take advantage of SPX. This utility enables a workstation to display the same information that appears on a NetWare server monitor. With the remote console software, the workstation user can execute server console commands without having to be at the server keyboard.

IPX/SPX can be deployed on a Microsoft network in one of two ways. One way is to install the ODI driver instead of NDIS at workstations and on pre-Windows 2000 servers. Because this offers limited 16-bit support, the better way is to use NetWare Link (NWLink). **NWLink** is a network protocol used on Microsoft networks via NDIS to emulate IPX/SPX.

The best way to install NWLink is to install it as part of Client Service for NetWare (CSNW), which installs three elements as follows (Figure 3-9 shows two of the three elements installed):

- Client Service for NetWare
- NWLink IPX/SPX/NetBIOS Compatible Transport
- NWLink NetBIOS

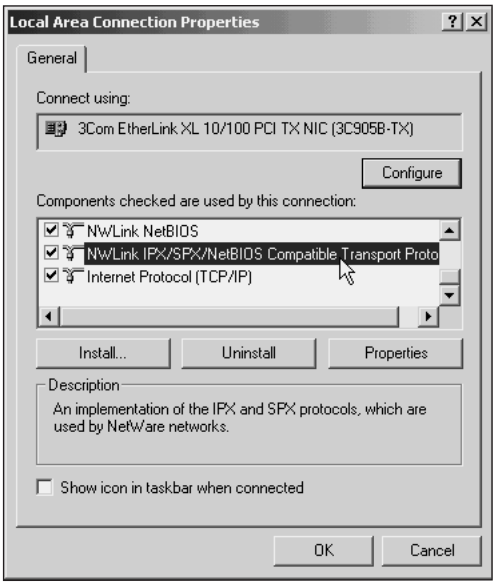

Figure 3-9 Windows 2000 with CSNW components installed

When you set up NWLink, you need to configure three elements in the process: the frame type, network number, and internal network number. In many situations, Windows 2000 automatically configures the frame type to match what is already in use by NetWare servers. The frame type determines how frames are formatted for NetWare communications. Windows 2000 also automatically configures the network number, or you can configure it by checking with the NetWare administrator. NetWare uses the network number, such as 1, to identify the network to which it is connected.

The internal network number is used to create a direct network route between a Windows 2000 server and a NetWare server in the following situations:

- When there are two or more frame types associated with the NetWare server you are accessing
- When your computer running Windows 2000 has two or more NICs, and NWLink is bound to more than one of these NICs
- When an application, such as a database, implements NetWare's Service Advertising Protocol (SAP) to identify a specific server

NWLink offers several advantages, such as routing over enterprise networks and the ability for Microsoft Windows-based operating systems to access NetWare servers as clients. NetWare clients, such as those that use NetWare Client32, can also access Windows 2000 servers. It is easy to install and provides more effective communication with NetWare file servers than does the ODI driver. NWLink supports WinSock and NetBIOS over IPX. NWLink also supports Microsoft's File and Print Services for NetWare (FPNW). When FPNW is installed in Windows 2000 Server, NetWare clients can access files, printers, and applications via the Windows 2000 Server. NWLink's disadvantages are that it is not as universal as TCP/IP and it is not transported as fast as NetBEUI. Also, IPX/SPX and the NWLink emulation are really designed as proprietary protocols used mainly on NetWare networks. Another disadvantage is that IPX/SPX is a "chatty" protocol in that each packet transmitted must be acknowledged by the receiving node.

The most common situations for using Microsoft's NWLink to emulate IPX/SPX are as follows:

- To enable a workstation running Microsoft Windows 95, Windows 98, Windows NT, or Windows 2000 to communicate with one or more NetWare servers (pre-version 5)
- To set up a Microsoft Windows NT or a Windows 2000 server as a gateway to one or more NetWare servers
- To enable NetWare clients to access a Windows 2000 server.

For example, assume that you are configuring workstations running Windows 98 for a network with five Novell NetWare servers and no other host computers. In this situation, you would configure all workstations to use NWLink. However, consider another situation where there is one NetWare 5.0 server and four Windows 2000 servers on a network, and some print services are to be handled through the Windows 2000 servers. One solution would be to configure all Windows-based workstations for NWLink and TCP/IP. Depending on the need for access to the NetWare server, a better solution would be to configure one of the Windows 2000 servers for NWLink and set it up to act as a gateway to NetWare by installing Microsoft's Gateway Service for NetWare. Now the workstations would only need to use TCP/IP, because they would access the NetWare server through the Windows 2000 Server gateway. In this instance, the gateway functions to make the NetWare directories appear as a shared folder on the Windows 2000 Server.

NetBIOS and NetBEUI

NetBIOS Extended User Interface (**NetBEUI**) is a communications protocol that is native to Microsoft network communication; however, with the release of Windows 2000, NetBEUI is not recommended over TCP/IP in most situations. First developed by IBM in 1985, it is an enhancement of **Network Basic Input/Output System** (**NetBIOS**). NetBIOS, which is not a protocol, is a method for interfacing software with network services. It also provides a naming convention.

NetBIOS

When a software application is written for compatibility with the NetBIOS interface, it calls the NetBIOS.dll file, which links the software to the transport driver. The transport driver communicates with NetBEUI for network transmissions. The transport driver used to interface with TCP/IP is called NetBIOS for TCP/IP (NetBT) and is contained in the file Netbt.sys. The driver that interfaces with NetBEUI and NetBIOS over IPX is NetBIOS.sys. Microsoft Windows 3.1, 3.11, 95, and 98 are most compatible with older programs requiring the NetBIOS interface. Windows NT and Windows 2000 use a NetBIOS emulator (a program that simulates NetBIOS) for communication between NetBIOS and NetBEUI. Figure 3-10 illustrates the communication flow from NetBIOS applications to NetBEUI, in order to transport data over a network.

You can find the Netbt.sys and NetBIOS.sys files in *Winnt\System32\Drivers*. Also, depending on which services are installed that use NetBIOS, you can find NetBIOS.dll in other system folders, such as \Winnt\System32\dllcache and \Winnt\System32\Netmon\Parsers.

NetBIOS names are used to name objects on a network, such as a workstation, server, or printer. For example, your workstation might use your favorite nickname for identification to other network users, the network printer you access might be named HPLaser, and the server you access might be named Netserver. These names make it easy for human beings to identify a particular network resource. They are translated into an address for network communications by the NetBIOS Name Query services.

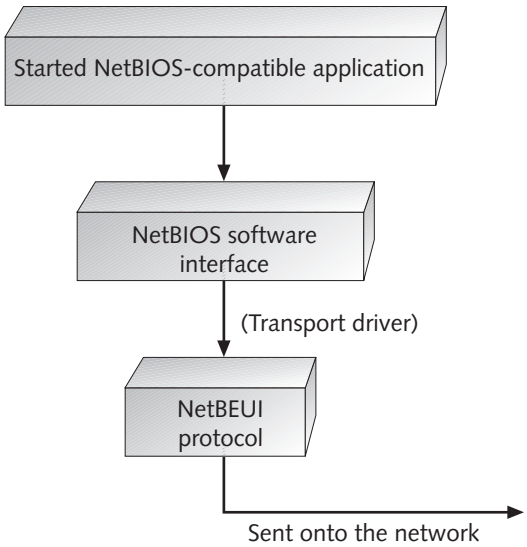

Figure 3-10 NetBIOS/NetBEUI communication

There are two important elements to remember about NetBIOS names. First, each name must be unique. No network object can have the same name as another object. If it could, there would be great confusion about how to communicate with objects having the same name. Second, names are no more than 16 characters. The first 15 characters are used by a user to assign a name, and the last character is used to identify the type of network resource, such as a server or printer, which the operating system handles using a hexadecimal number.

NetBEUI

NetBEUI was developed when computer networking primarily meant local area networking for a relatively small number of computers (generally, from a couple of computers to about 200). It was not developed to take into account enterprise networks, in which packets are directed from one network to another through routing and routers. For this reason, NetBEUI is suited for small LANs using older Microsoft or IBM server operating systems such as Microsoft LAN Manager and IBM LAN Server.

Advantages and Disadvantages of NetBEUI

NetBEUI is a good choice on small Microsoft networks running only Windows-based clients and a combination of Windows 2000 and Windows NT servers, for several reasons. First, it is simple to install, and it is very compatible with Microsoft workstation and server operating systems. Second, it can handle nearly limitless communication sessions on one network, because the 254-session limitation of earlier versions is removed. Microsoft specifications, for example, show that a Windows server can support 1000 sessions on one NIC. Third, NetBEUI has low memory requirements and can be quickly transported over small networks. Fourth, it has solid error detection and recovery. Fifth, it is self-configuring and self-tuning. Last, it can provide both connection-oriented and connectionless communications.

The inability to route NetBEUI is a major disadvantage for medium and large networks, including enterprise networks. This means a NetBEUI frame cannot be forwarded by a router from one network to another, because there is not enough information in the NetBEUI frame to identify specific networks. When NetBEUI is used over two or more LANs that are connected together, the LANs must be connected by **bridge** devices, which operate at a lower communication level (OSI Layer 2) than routers (OSI Layer 3) and do not look for routing information. Or, routers that can be set to route or bridge (called brouters) must be set in bridge mode to forward NetBEUI frames from one network to another, resulting in extra total network traffic. Another disadvantage is that there are fewer network analysis tools for it than for other protocols. NetBEUI also is not widely supported by computers running non-Microsoft operating systems and it is limited to small LANs. Last, NetBEUI is chatty, because it sends out more broadcast traffic than TCP/IP (but not more than IPX/SPX).

Consider two different networking situations. In the first situation, you are responsible for setting a up network for a credit union that has 52 workstations, four network printers, no routers, no outside connections to other networks, and one Microsoft NT server. This is a good context for using NetBEUI as the sole protocol. In a second situation, you are setting up communication on a busy college network with 520 nodes, including an IBM

mainframe, 10 Windows 2000 servers, and Internet access. That network has four routers linking different LANs across campus. NetBEUI is not a good choice in this situation because it cannot route. TCP/IP is the best alternative because it has routing capabilities and IP addressing for Internet access.

DLC

When it is not possible to connect to an IBM mainframe using TCP/IP, another way to connect is to use the **Data Link Control** (**DLC**) **protocol**. Microsoft Windows NT, Windows 2000, Windows 95, and Windows 98 offer a DLC driver that can be installed. DLC provides the ability to connect to IBM's older network communications system, called Systems Network Architecture (SNA). Another use for DLC is to communicate with printers directly connected to the network, such as a Hewlett Packard 4Si laser printer equipped with print services and network connectivity.

The main advantage to using DLC is that it is an alternative to TCP/IP when TCP/IP is not available. The disadvantages are that the protocol is not routable. Also, DLC is not truly designed for peer-to-peer communication between workstations, but only for connectivity to a computer such as an older IBM ES9000 mainframe or AS/400 minicomputer, or connectivity to a peripheral device that uses DLC.

AppleTalk

Macintosh computer networks use a peer-to-peer network protocol called **AppleTalk**. AppleTalk is only supported in very limited ways on non-Macintosh networks. On a Microsoft network, Macintosh computers are linked in by setting up the Windows 2000 Server Services for Macintosh, which include the following components:

- File Server for Macintosh (MacFile)
- Print Server for Macintosh (MacPrint)
- AppleTalk protocol

Using MacFile, the Windows 2000 Server becomes a file server for Macintosh computers as well as for computers running Microsoft operating systems. Through MacPrint and AppleTalk, Macintosh clients can print documents on network printers that are managed by a Windows 2000 server, and non-Macintosh clients can print files on printers shared by Macintosh computers. The Services for Macintosh also include the ability to route AppleTalk and to set up remote access for Macintosh computers via modem and telephone lines.

Protocol Binding Order

When a network uses multiple protocols for communication among servers, workstations, and printers, some network operating systems, Windows NT and Windows 2000 for example, have the ability to establish an order in which protocols are bound to a NIC. Setting the binding order for file and print services is one way to inexpensively improve network performance. The binding order is most important on workstations when they attempt to connect to a server. For

example, your network might contain 20 Windows 2000 servers configured for TCP/IP and two NetWare 4.0 servers configured for IPX/SPX. On this network there are over 1000 Windows NT and Windows 2000 workstations that access the servers and are configured to use both TCP/IP and NWLink. The workstations primarily access the Windows 2000 servers and network printers using TCP/IP. In this situation you can dramatically improve network performance by setting up each workstation so that TCP/IP is first in the binding order, and NWLink is second. This means that each workstation will first use TCP/IP when it attempts to connect to a server, instead of first attempting to connect through NWLink and then sending another connection attempt using TCP/IP. On a busy network with over 1000 workstations and on which all of the users start to log on to servers at 8 a.m. when they come to work, this simple adjustment can reduce the morning network traffic by half. (You can practice setting the binding order in Hands-on Projects 3-6 and 3-7. Also, try Hands-on Project 3-8 to unbind a protocol.)

It is helpful to set the binding order on Windows NT and Windows 2000 servers, but the gain is not as dramatic in terms of network performance as it is for workstations. This is because there are fewer servers than workstations, and generally the servers remain logged on to the network.

In Windows NT and Windows 2000, the binding order can be set for both file services and print services; in some cases, the binding order will not be the same for both. For example, TCP/IP may be used for file services on Windows 2000 servers, and IPX/SPX may be used for print services managed through a NetWare server. In this case, you would set TCP/IP to have the first binding order for file services, and NWLink to be first for print services.

Planning a Network

Before you begin implementing Windows 2000 Server and deciding upon which protocols are needed, analyze your network requirements and develop a network plan. The first step in network planning is to assess the business or organizational needs for which the network is to be used. These include the following:

- Size and purpose of the organization
- Potential growth of the organization in terms of people and services
- Number of mission-critical applications on the network
- Important cycles for the business or organization
- Relationship of the network resources to the mission of the business or organization
- Security needs
- Amount budgeted for network and computer resources

- Internet and intranet requirements
- Interconnectivity needed to other computers, such as IBM mainframes, Macintosh computers, and NetWare servers

There are many other considerations, but these provide a good start. For example, if you are working with a large organization that is likely to grow, there will be a particular emphasis on planning how to implement TCP/IP and its associated protocols. For a small network, such as a 15-person dental office, the network design needs to be reliable, and easy to manage on a small budget. NetBEUI may be a good choice for this network, if there are no routers and no plans for Internet connectivity.

Some organizations, such as accounting and payroll departments or banks, work with very sensitive financial information, requiring a high degree of reliability, security, and fault tolerance. Also, those organizations have especially urgent cycles of business activity, including daily electronic transmissions of money, daily account balancing, month-end and year-end accounting cycles, income tax reporting, and regular audits from independent financial auditors. Your network planning and management must always take into account those important business cycles. For example, you do not want to convert from NetBEUI to TCP/IP in the middle of year-end processing or just before an electronic transmission to the Federal Reserve.

In many cases, the network and computing resources are a cornerstone in the business strategy of an organization. A president of a subscription company that markets collectible items regards the computer capabilities of his company as the key reason the company stays ahead of the competition. Computing resources enable that company to provide the fastest customer service and delivery of products. When a customer places an order, a series of inventory, billing, customer profiling, promotional, manufacturing, and product-shipping events occurs automatically through the computer systems. For colleges, computer systems play an important role in attracting and retaining students, for example recruiting, admitting, and registering students, and providing grade and degree progress information. In these situations the versatility of TCP/IP and QoS may be important. Also, on a college campus that has Macintosh labs, the ability to configure AppleTalk is vital.

At one time, security was not a priority on many computers and networks, because few people knew how to intrude into systems. Times have changed, and responsible network planning always includes a blueprint for security. Besides guarding against intrusions, security also includes backing up data, planning for computer failures, and having a plan for disaster recovery. If security is important in your implementation, consider the ability to set up subnets and routers.

From the start, learn how the network is related to the needs of its users, determine what resources already exist, and plan a secure network positioned for growth. A given in networking is that once a network is successfully implemented and managed, the requests to expand its capabilities start immediately.

Selecting the Right Protocol

The protocols you employ on a network depend on several factors:

- Do packets need to be routed?
- Is the network small (20 or so connections), medium (100 to 500 connections), or large (over 500 connections)?
- Are there Microsoft 2000 servers?
- Are there mainframe host computers, and do they use SNA?
- Are there NetWare servers?
- Is there direct access to the Internet or to Web-based intranet applications?
- Are there mission-critical or multimedia applications?

If there is a need to route packets, such as on an enterprise network, your best choice is likely to be TCP/IP because it is designed for routing and it is used on many types of networks. For a small nonrouted network with only Microsoft servers and workstations, NetBEUI can be a good choice as long as there is no Internet or intranet activity. A network with a combination of NetWare (pre-version 5) and Windows 2000 servers will need to employ TCP/IP and NWLink, whereas a network with only NetWare 5.x servers and Windows 2000 servers can use TCP/IP as the sole protocol.

Connectivity to Internet or Web-based services requires that TCP/IP be implemented and that FTP services be used to transfer files. TCP/IP also is the first choice for connectivity to mainframe and UNIX computers. The Telnet terminal emulation available through TCP/IP may be needed to connect to the mainframe. DLC is another option for IBM mainframe and minicomputer communications, if TCP/IP cannot be used.

TCP/IP is the protocol of preference for medium to large-sized networks. It can be routed, is reliable for mission-critical applications, and has solid error checking. Network monitoring and analysis becomes very important on these networks, and TCP/IP has associated protocols to accomplish these activities, too. Also, any network that uses multimedia applications and multicasting should employ TCP/IP.

In many cases it is necessary to use a combination of protocols to accommodate different types of network applications. Modern networks often use combinations of the major protocols, TCP/IP, NetBEUI, and IPX/SPX. However, remember that it is best to use only those protocols that are required, because the more protocols that are transported, the more drain there is on network performance.

Sample Planning Scenarios

Consider that you are selecting a protocol for a college network that uses Windows 2000 Server, uses routing to several buildings, employs multimedia applications, has Internet connectivity, and uses Windows 98 for 700 clients. In this situation, TCP/IP can be used alone. TCP/IP offers several advantages, including the ability to route packets and use of RSVP

and QoS to allocate resources for multimedia. In this situation, TCP/IP also provides Internet accessibility for research and e-mail, and supports HTTP for Web browser use.

In another scenario, you are planning a network for a company that has five NetWare 3.0 and 4.0 servers and eight Windows 2000 servers. Also, you want to set up a Windows 2000 gateway to one of the NetWare servers, and there is an IBM mainframe that is set up only for SNA connectivity. In this situation, you will likely need to set up NWLink on the Windows 2000 servers for connectivity to NetWare, DLC to connect to the IBM mainframe, and TCP/IP for connectivity between the Windows 2000 servers and their clients. As part of the planning, you will need to determine which resources are used most frequently by which Windows NT Workstation and Windows 2000 Professional clients. For example, the business office workstations may access the Windows 2000 servers most, the mainframe next most frequently, and the NetWare servers least. Their workstations should be set up to have a binding order of TCP/IP, DLC, and NWLink. Or, if they will only access the one NetWare server via the Windows 2000 gateway, then those workstations only need TCP/IP and DLC, bound in that order.

In a third scenario, you have a network that contains four NetWare 4.0 servers set up for IPX/SPX communication. The decision is made to upgrade the NetWare servers to version 5.0. Also, your organization has purchased a new client/server system that requires three Windows 2000 servers. To reduce the number of protocols needed on the network, you should plan to convert the NetWare servers and clients to TCP/IP and to set up TCP/IP on the new Windows 2000 servers.

In a last scenario, there is an office of 22 tax accountants, who have a small network without routers. Each accountant has a Windows 98 computer, and there is one Windows 2000 server. Also, one of the accountants has Internet access through a modem on her workstation. This is a situation in which NetBEUI is effective and easy to manage. Only the workstation that has Internet connectivity needs to be configured for TCP/IP. However, if there is a plan to have Internet connectivity for all network users via the server, then TCP/IP can be used instead of NetBEUI for all workstations and the server.

Chapter Summary

- Protocols are the heart of network communications. Just as life would be silent without language, networks would be silent without protocols. Because protocols are vital to network communication, your first step in setting up a network that uses Windows 2000 is to plan how to set up the network and implement the right protocols. Different protocols are used for different kinds of networks such as LANs and WANs. Protocols also influence how you set up a network interface card and network client workstations.
- Network operating system vendors establish specifications for network drivers to enable protocol transport on a network. Microsoft uses the NDIS driver, which is fundamental to communication on Microsoft networks. Through the NDIS driver, Microsoft supports single to multiple protocol communications for TCP/IP, IPX/SPX, NetBEUI, DCL, and AppleTalk. Because so many networks use Internet and intranet connectivity, TCP/IP is generally the protocol of choice when you set up Windows 2000 Server.

TCP/IP is preferred because it provides reliable communication, IP addressing, and a suite of associated protocols that support many kinds of network functions.

- As you plan a network, carefully plan which protocols are needed to match what your organization wants to accomplish through the network. Also, keep two goals in mind: to use only those protocols that are necessary and to tune network performance through the protocol access order. Your thorough planning before setting up Windows 2000 Server and its associated network can be the cornerstone for having a successful and efficient network within a reasonable budget.

In the next chapter you are introduced to the Active Directory and learn how to plan its use for different types of situations.

KEY TERMS

Address Resolution Protocol (**ARP**) — A protocol in the TCP/IP suite that enables a sending station to determine the MAC address of another station on a network.

AppleTalk — A peer-to-peer protocol used in network communication between Macintosh computers.

bridge — A network transmission device that connects together different LAN segments using the same access method, for example connecting an Ethernet LAN to another Ethernet LAN or a token ring LAN to another token ring LAN. Bridge devices look at MAC addresses (OSI Layer 2) but do not look at routing information (Layer 3) in a frame.

connectionless communication — Also called a connectionless service, a communication service that provides no checks (or minimal checks) to make sure that data accurately reaches the destination node.

connection-oriented communication — Also called a connection-oriented service, this service provides several ways to ensure that data is successfully received at the destination, such as requiring an acknowledgement of receipt and using a checksum to make sure the packet or frame contents are accurate.

Data Link Control protocol (**DLC**) — Available through Microsoft Windows 2000, Windows NT, Windows 95, and Windows 98, this protocol enables communication with an IBM mainframe or minicomputer.

device address — Same as *physical address.*

Domain Name Service (**DNS**) — A TCP/IP application protocol that resolves domain and computer names to IP addresses, or IP addresses to domain and computer names.

dotted decimal notation — An addressing technique that uses four octets, such as 100000110.11011110.1100101.00000101, converted to decimal (For example, 134.22.101.005), to differentiate individual servers, workstations, and other network devices.

dynamic addressing — An addressing method whereby an Internet Protocol (IP) address is assigned to a workstation without the need for the network administrator to manually set it up at a workstation.

Dynamic Host Configuration Protocol (**DHCP**) — A network protocol that provides a way for a server to automatically assign an IP address to a workstation on its network.

enterprise network — A network that often reaches throughout a large area, such as a college campus, a city, or across several states. The main distinguishing factor of an enterprise network is that it brings together an array of network resources such as many kinds of servers, mainframes, intranets, printers, and the Internet.

Ethernet — A network transport system that uses a carrier sensing and collision detection method to regulate data transmissions.

File Transfer Protocol (**FTP**) — Available through the TCP/IP protocol, FTP enables files to be transferred across a network or the Internet between computers or servers.

frame — A unit of data that is transmitted on a network; it contains control and address information, but not routing information.

Hypertext Transfer Protocol (**HTTP**) — A protocol in the TCP/IP suite that transports HTML documents over the Internet (and through intranets) for access by Web-compliant browsers.

Internet Control Message Protocol (**ICMP**) — A TCP/IP-based protocol that is used for network error reporting, particularly through routing devices.

Internet Group Management Protocol (**IGMP**) — Part of the TCP/IP protocol suite, the protocol that is used in multicasting and which contains addresses of clients. It is used by the server to tell a router which clients belong to the multicast group.

Internet Packet Exchange (**IPX**) — A protocol developed by Novell for use with its NetWare Server operating system (see Sequence Packet Exchange).

local area network (**LAN**) — A series of interconnected computers, printers, and other computer equipment that share hardware and software resources. The service area is usually limited to a given floor, office area, or building.

media access control (**MAC**) **sublayer** — A network communications function that examines physical address information in frames and controls the way devices share communications on a network.

metropolitan area network (**MAN**) — A network that links multiple LANs within a large city or metropolitan region.

NetBIOS Extended User Interface (**NetBEUI**) — A communication protocol native to Microsoft network communications. It is an enhancement of NetBIOS, and was developed for network peer-to-peer communication among workstations with Microsoft operating systems installed on a local area network.

NetWare Link (**NWLink**) — A network protocol that simulates the IPX/SPX protocol for Microsoft Windows 95, Windows 98, Windows NT, and Windows 2000 communication with Novell NetWare file servers and compatible devices.

Network Basic Input/Output System (**NetBIOS**) — A combination software interface and a network naming convention. It is available in Microsoft operating systems through the file, NetBIOS.dll.

network binding — A process that links a computer's network interface card or a dial-up connection with one or more network protocols to achieve optimum communication with network services. For Microsoft operating systems, you should always bind a protocol to each NIC that is installed.

Network Driver Interface Specification (**NDIS**) — A set of standards developed by Microsoft and 3COM for network drivers that enables communication between a NIC and a protocol, and that enables the use of multiple protocols on the same network.

Open Datalink Interface (**ODI**) — A driver that is used by Novell NetWare networks to transport multiple protocols on the same network.

Open Shortest Path First (**OSPF**) **protocol** — A TCP/IP-based routing protocol that can evaluate network paths and match a type of transmission, such as data or video, to the appropriate network path.

packet — A unit of data that is transmitted on a network, and contains control and address information as well routing information.

physical address — Also called a device address, a unique hexadecimal number associated with a device's network interface card.

protocol — A strictly defined set of rules for communication across a network that specifies how networked data is formatted for transmission, how it is transmitted, and how it is interpreted at the receiving end.

Quality of Service (**QoS**) — Mechanisms used to measure and allocate network resources on the basis of transmission speed, quality, throughput, and reliability.

Resource Reservation Protocol (**RSVP**) — Enables an application to reserve the network resources it needs, such as network paths with higher speeds.

router — A device that connects networks, that can read IP addresses, and that can route packets to designated networks, because it reads routing information in packets (Layer 3) and keeps tables of information about the fastest route from one network to another.

Routing Information Protocol (**RIP**) — A TCP/IP-based protocol that enables routing devices to share information about a network.

Sequence Packet Exchange (**SPX**) — A Novell connection-oriented protocol used for network transport when there is a particular need for data reliability (see Internet Packet Exchange).

Simple Mail Transfer Protocol (**SMTP**) — An e-mail protocol used by systems having TCP/IP network communications.

Simple Network Management Protocol (**SNMP**) — A TCP/IP-based protocol that enables servers, workstations, and network devices to gather standardized data about network performance and identify problems.

static addressing — An IP (Internet Protocol) addressing method that requires the network administrator to manually assign and set up a unique network address on each workstation connected to a network.

subnet mask — A designated portion of an IP address that is used to indicate the class of addressing on a network and to divide a network into subnetworks as a way to control traffic and enforce security.

Telnet — A TCP/IP application protocol that provides terminal emulation services.

token ring — Using a ring topology, a network transport method that passes a token from node to node. The token is used to coordinate transmission of data, because only the node possessing the token can send data.

topology — The physical layout of the cable and the logical path followed by network packets and frames sent on the cable.

Transmission Control Protocol/Internet Protocol (**TCP/IP**) — A protocol that is particularly well suited for medium and large networks. The TCP portion was originally developed to ensure reliable connections on government, military, and educational networks. It performs extensive error checking to ensure data is delivered successfully. The IP portion consists of rules for packaging data and ensuring it reaches the correct destination address.

User Datagram Protocol (**UDP**) — A protocol used with IP as an alternative to TCP and that offers low-overhead connectionless communications.

wide area network (**WAN**) — A far-reaching system of networks that can extend across state lines and across continents.

Windows Internet Naming Service (**WINS**) — A Windows 2000 Server service that enables the server to convert workstation names to IP addresses for Internet communication.

Review Questions

1. You are setting up a bridged network between two floors in a small office building that has one Windows 2000 server and 42 users who run Windows 95 and Windows 98. Can you implement NetBEUI as a protocol on this network?
   a. Yes
   b. No
   c. NetBEUI can be implemented as long as you use NWLink for network print services.
   d. NetBEUI can be implemented, but you must use DLC for any workstation that connects to the Internet.
2. What protocol enables a DHCP server to determine the IP and physical addresses of a client that has just joined the network?
   a. NetBIOS
   b. RIP
   c. ARP
   d. all of the above
   e. only a and b
   f. only a and c
3. Which of the following network driver specifications enable(s) you to transport two or more protocols on the same network?
   a. NDIS
   b. ODI
   c. ARP
   d. all of the above

e. only a and b

f. only a and c

4. You work for a news organization that offers multimedia news clips over the Internet via a Windows 2000 Web server. You have several Internet network connections, some of which are high-speed and some of which are not. Which of the following TCP/IP capabilities might be useful to you?

   a. RSVP

   b. multicasting

   c. QoS

   d. all of the above

   e. only a and b

   f. only b and c

5. You are setting up a new network that uses two Windows 2000 servers for a business and accounting system that will be available for administrative use at a community college. Only 20 users will access the system in the first two months. Gradually more users will go onto the system, until there are 322 within 12 months. All of the client workstations are Windows 2000 Professional and Windows 98. What protocol will you set up?

   a. NetBEUI for the first year and then convert to TCP/IP when you know the system is working properly

   b. TCP/IP from the beginning

   c. UDP/IP for fastest response

   d. UDP for the first two months and then convert to TCP when you know the system is working properly

6. Which of the following is (are) available through AppleTalk?

   a. file services

   b. print services

   c. peer-to-peer networking

   d. all of the above

   e. only a and b

   f. only a and c

7. You are manually setting up TCP/IP on your Windows 2000 server. Which configuration elements must you establish to communicate on the network?

   a. a WINS server address

   b. an IP address

   c. a subnet mask

   d. all of the above

   e. only a and b

   f. only b and c

8. You have a network that contains both Windows 2000 servers and NetWare 5.0 servers as the main host computers accessed by Windows 95, Windows 98, and Windows 2000 workstations. Which of the following protocols do you need to set up?
   a. NetBEUI
   b. NWLink
   c. TCP/IP
   d. all of the above
   e. only a and c
   f. only b and c
9. One important difference between TCP and UDP is that
   a. TCP contains source and destination addresses and UDP does not.
   b. TCP is connection-oriented and UDP is not.
   c. UDP is connection-oriented and TCP is not.
   d. UDP cannot be routed, but TCP can.
10. A NIC contains which of the following?
    a. transmitter
    b. serial bus
    c. power supply
    d. all of the above
    e. only a and b
    f. only a and c
11. Which of the following is (are) part of the QoS implementation in Windows 2000?
    a. Prioritized LANs
    b. Address Resolution Protocol
    c. Admission Control Service
    d. all of the above
    e. only a and b
    f. only b and c
12. 155.242.1.299 is an example of what type of address?
    a. MAC
    b. dotted decimal
    c. physical
    d. subaddress

13. Your TCP/IP-based network seems to have some problems with slowdowns. Which of the following protocols might help you gather information about network performance and locate the problem?
    a. SNMP
    b. DNS
    c. DHCP
    d. all of the above
    e. only a and b
    f. only b and c
14. Your network consists of four Windows 2000 servers, a mainframe, 20 networked Hewlett Packard 4Si printers, and 122 workstations that run Windows 2000 Professional. The workstations primarily access the Windows 2000 servers and are configured for TCP/IP, NetBEUI, DLC, and NWLink. Communication with the servers is via TCP/IP and communication with the mainframe and network printers is through DLC. Network performance does not seem to be as fast as you would like it. What simple step(s) might you take to improve network performance?
    a. Convert all communications to NetBEUI.
    b. Eliminate the use of NWLink and NetBEUI.
    c. Check the network access order at the workstations.
    d. Convert all communication to DLC because it has low overhead.
    e. only a and c
    f. only b and c
15. Which of the following protocols cannot be routed?
    a. IPX/SPX
    b. NWLink
    c. NetBEUI
    d. TCP/IP
16. As you are planning the setup of Windows 2000 servers on a routed network using TCP/IP, you realize that setting up TCP/IP on all 272 workstation clients will require lots of manual labor. What can you do to reduce your workload?
    a. turn off routing
    b. use DHCP and set up one of the Windows 2000 servers as a DHCP server
    c. set up one of the Windows 2000 servers as a DNS server
    d. use RIP at the routers instead of SMTP

17. What type of address is burned into a NIC?
    a. MAC
    b. IP
    c. NetBEUI
    d. HTTP
18. Which type of packet can be used to send fewer network transmissions for a multimedia presentation over a network?
    a. unicast
    b. multicast
    c. broadcast
    d. frame
19. Which of the following contains routing information?
    a. frame
    b. packet
    c. bus
    d. MAC sublayer
20. When you bind a protocol, you bind it to
    a. a driver
    b. a computer bus
    c. a NIC
    d. a WINS server
21. Which TCP/IP-based protocol is needed for Web communications that involve HTML?
    a. Telnet
    b. SMTP
    c. HTTP
    d. WWW
22. 255.255.0.0 is an example of
    a. a device address
    b. a binding number
    c. a DNS server address
    d. a subnet designation
23. NetBIOS is
    a. an interface
    b. a protocol

c. a socket

d. a topology

24. You are configuring routers to communicate with one another. Which of the following TCP/IP-based protocols might you use?

a. RIP

b. FTP

c. SMTP

d. all of the above

e. only a and b

f. only a and c

25. Originally your network was small and relied on a network service provider to provide translation of IP addresses to computer names. Now you have a larger operation and want to place this function on your own network. Which Windows 2000 capability enables you to do this?

a. DLC server

b. DNS server

c. Active Directory

d. bridging

HANDS-ON PROJECTS

Project 3-1

In this project, you check to make sure that the NIC in a computer running Windows 2000 is working properly. You will need an account with Administrator privileges.

To check on the NIC:

1. Log on to Windows 2000 Server.
2. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**.
3. Right-click **Local Area Connection** and then click **Properties**. Make sure you are viewing the General tab.
4. What type of NIC is installed in your computer?
5. Click the **Configure** button.
6. Click the **General** tab.
7. What does the Device status text box say about how the NIC is working?
8. Record the information that you obtain in your lab journal or in a word-processed document.

9. Click **Cancel** to close the NIC's Properties dialog box.
10. Click **Cancel** to close the Local Area Connection Properties dialog box.
11. Close the Network and Dial-up Connections dialog box, if it has remained open.

Project 3-2

In this hands-on activity you determine the physical (MAC) address of the NIC in a Windows 2000 server. (This project will also work using Windows 2000 Professional).

To determine the physical address:

1. Log on to Windows 2000.
2. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
3. Type **ipconfig /all** and press **Enter** at the command prompt (see Figure 3-11).
4. Notice the physical address of the NIC.
5. Is there an IP address assigned?
6. What is the description of the NIC?
7. Is there a DNS server on your network? If so, what is its IP address?
8. What other information is available from using Ipconfig?
9. Record the information that you obtain in your lab journal or in a word-processed document.
10. Close the Command Prompt window.

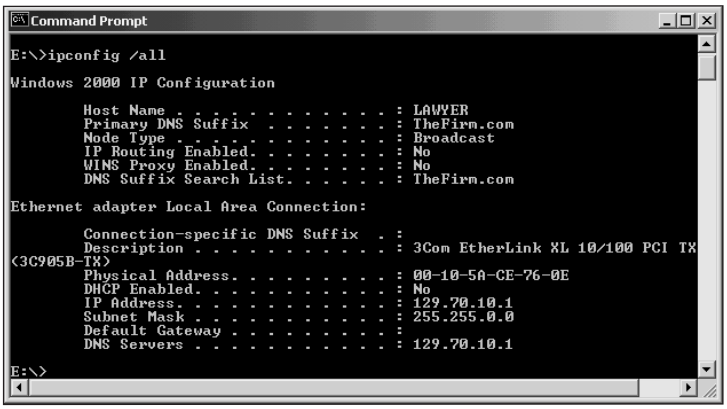

Figure 3-11 Using Ipconfig

Project 3-3

In this project, you practice another way to view a physical address in Windows 2000 Server.

To view the physical address:

1. Log on to Windows 2000, if you logged off after Hands-on Project 3-2.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Computer Management**.
3. Click **System Information** in the left pane under **System Tools**.
4. Double-click **Components** in the right pane.
5. Double-click **Network** in the right pane and double-click **Adapter**.
6. Notice the value of the MAC address and compare it with the MAC address you obtained in Hands-on Project 3-2. What other information is available on this screen?
7. Close the Computer Management tool.

Project 3-4

This hands-on activity enables you to practice converting a server running Windows NT 4.0 to TCP/IP as preparation for upgrading to Windows 2000 Server. You will need an account with Administrator privileges. Also, obtain an IP address and subnet mask to use from your instructor.

To set up TCP/IP in Windows NT 4.0 before converting to Windows 2000:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network** icon.
3. Click the **Protocols** tab in the Network dialog box, then click **Add**.
4. Highlight the **TCP/IP Protocol** option and then click **OK**.
5. Determine if there is a Windows NT DHCP server on the network. If there is one, click Yes, otherwise click No. For this practice session, click **No**.
6. Insert the Windows NT Server CD-ROM as requested, enter the path to the CD-ROM drive and \I386, and click **Continue**. (If Remote Access Service is installed, there is a dialog box that enables you to click Yes or OK, depending on your service pack level, to configure for this service).
7. The installation program returns to the Protocols tab after the files are loaded. Click the **Bindings** tab to automatically configure the NIC for TCP/IP.
8. Click the **Protocols** tab, point to **TCP/IP Protocol**, and then click the **Properties** button.
9. Click the **IP Address** tab and then enter the IP address and the network subnet mask.
10. If there is a DNS server, click the **DNS** tab and complete the Host Name and Domain text boxes. Click **Add** under DNS Service Search Order, enter the address of the DNS Server (obtain this from your instructor), and click **Add**. Click **Apply** and then **OK**.

11. If there is a WINS server, click the **WINS Address** tab and then enter the addresses of the primary and secondary WINS servers. Also, if you specified a DNS server, click the box, **Enable DNS for Windows Resolution**. Click **Apply** and then **OK**.
12. Click **Close** in the Network dialog box.
13. Windows NT will perform a binding review.
14. If necessary, save any open work, then click **Yes** to restart the computer to have the new protocol take effect.

Project 3-5

In this hands-on activity, you experiment with the Ping utility, which uses ICMP. Before you start, obtain from your instructor two addresses to Ping, one that is an IP address on your local network and the other an IP address on a distant network connected to your campus or on the Internet. You can use either Windows 2000 Server or Windows 2000 Professional for this assignment.

To use Ping:

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. Type **Ping** and the IP address of the local network node (or type the address of your node if you found one in Hands-on Project 3-1). What information is produced from using Ping?
3. Type **Ping** and the IP address of the distant node. Is the node responding? What information do you see?
4. If you obtained a DNS server address from Hands-on Project 3-1, Ping it to see if it is responding.
5. Record the information that you obtain in your lab journal or in a word-processed document.
6. Close the Command Prompt window.

Project 3-6

In this hands-on activity, you set the binding order in Windows NT 4.0 (you do the same thing for Windows 2000 in the next project). You will need a computer running Windows NT 4.0 Workstation or Server that is configured for at least two network providers (protocols) and two print providers, and access to an account with Administrator privileges.

To set the binding order in Windows NT 4.0:

1. Log on to Windows NT.
2. Click **Start**, point to **Settings**, and then click **Control Panel**.
3. Double-click the **Network** icon and then click the **Services** tab.
4. Click the **Network Access Order** button.

5. Under Network Providers, click the network type or protocol listed second and then click **Move Up**.
6. Under Print Providers, click the network type or protocol listed second and then click **Move Up**.
7. Click **OK** and then click **Close**.
8. Click **Yes** to restart the computer (save any open work first).

Project 3-7

In this project, you change the network access order in Windows 2000 Server or Windows 2000 Professional. The operating system should already be configured for two network and print providers and you will need access to an account with Administrator privileges.

To change the network access order in Windows 2000 Server or Professional:

1. Log on to Windows 2000.
2. Right-click **My Network Places** on the desktop and then click **Properties** on the menu.
3. Click the network connection that you want to change — ask your instructor which connection to use or click **Local Area Connection**.
4. Click **Advanced** on the menu bar in the Network and Dial-up Connections dialog box.
5. Click **Advanced Settings** on the Advanced menu.
6. Click the **Adapters and Bindings** tab to view the current bindings (see Figure 3-12). What bindings exist on your computer?

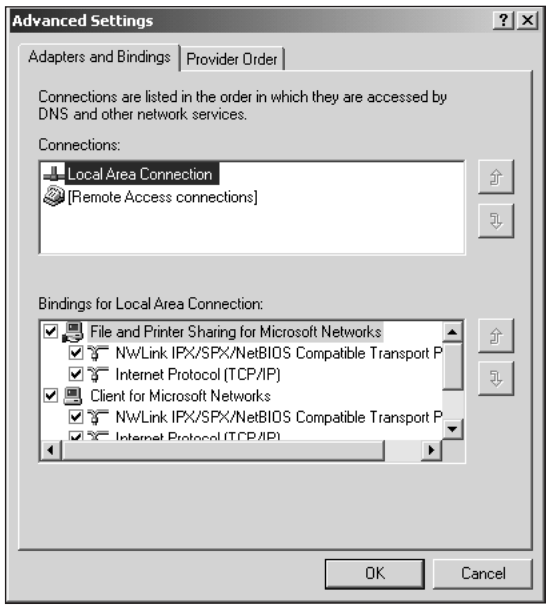

Figure 3-12 Bindings in Windows 2000

7. Click the **Provider Order** tab.
8. Under Network Providers, click the network type or protocol listed second and then click the up arrow button.
9. Under Print Providers, click the network type or protocol listed second and then click the up arrow button.
10. Click **OK**.
11. Close the Network and Dial-up Connections dialog box.
12. If you are keeping a lab journal, note that you do not have to restart Windows 2000 to change the access order, whereas you did have to restart Windows NT in the previous hands-on project. Also, make a note of the differences between what is displayed for network bindings and access order between Windows NT 4.0 and Windows 2000. In addition, note how you accessed the Network and Dial-Up Connections dialog box in this project compared to how you accessed it in Hands-on Project 3-1.

Project 3-8

In this project, you practice removing NWLink from the access order in Windows 2000 by unbinding it. You will need a Windows 2000 server or workstation that has NWLink installed before you start.

To unbind NWLink:

1. Log on to Windows 2000.
2. Right-click **My Network Places** on the desktop and then click **Properties** on the menu.
3. Click the network connection that you want to change — ask your instructor which connection to use or click **Local Area Connection**.
4. Click **Advanced** on the menu bar in the Network and Dial-up Connections dialog box.
5. Click **Advanced Settings** on the Advanced menu.
6. Click the **Adapters and Bindings** tab to view the current bindings.
7. Under File and Printer Sharing for Microsoft Networks, click the check box to the left of NWLink IPX/SPX/NetBIOS Compatible Transport Protocol to remove the check.
8. Under Client for Microsoft Networks, also click the check box to the left of NWLink IPX/SPX/NetBIOS Compatible Transport Protocol to remove the check.
9. Click **OK**.
10. Close the Network and Dial-up Connections dialog box.
11. Make a note in your lab journal that it is not necessary to reboot Windows 2000 to unbind a protocol.

CASE PROJECT

Aspen Consulting Project: Protocol Planning and Implementation

Batesberg College is a liberal arts college that has 742 students, 51 faculty, and a staff of 43. There are eight buildings on campus that serve as classrooms and offices. Three additional buildings are dorms. All buildings are networked via Ethernet and connected by brouters (routers that can be set up to bridge or route) in each building. There is a computer machine room in the basement of the Administration Building that houses the following:

- A UNIX computer that is used for administrative computing, including registration
- Seven Novell NetWare 3.11 servers that support the faculty, which are used by student labs throughout campus, and which are set up for IPX/SPX
- Two Windows NT 4.0 servers set up to use NetBEUI and TCP/IP — one server is used for a client/server system for the Development Office, and one is a Web server

Five of the classroom buildings house student labs, with one lab in each. Four of the labs consist of computers running Windows 95 and Windows 98. The fifth lab consists of Macintosh computers that do not connect to any server, but use peer-to-peer networking. All of the student dorms provide Ethernet network access. The Development Office has just completed a fund-raising campaign to upgrade computer facilities. The campus computer planning committee has mandated that four of the NetWare servers will be converted to Windows 2000 Server, and the remaining three will be upgraded to NetWare 5.0. Also, the Windows NT 4.0 servers will be upgraded to Windows 2000 Server.

1. What preparations do you recommend to the Batesberg College Information Technology Department in terms of preparing the Windows NT 4.0 servers for the upgrade to Windows 2000? Why?
2. The Windows 2000 workstations in the Registrar's Office are set up to use TCP/IP, NWLink, and AppleTalk. These workstations are used to access the UNIX computer and the Web server only. Which of these protocols is really needed for the workstations, and should the workstations be set up to take advantage of access order? Explain your answer.
3. The Journalism Department uses the Macintosh lab to teach students about different types of publication software. They want students to be able to connect to one of the new Windows 2000 servers for lab use. What are their options for connecting to one of these servers?
4. The Chemistry, Math, Sociology, and Zoology departments want to use simulated multimedia lab presentations that will run to the labs and dorms from two of the new Windows 2000 servers. What server capabilities will help make multimedia use a reality?

5. After all of the server upgrades are made, and considering the requests presented in Questions 3 and 4, what protocols do you recommend for the entire campus network? Note that the IT director likes NetBEUI for Windows 2000 servers because he believes it creates the lowest overhead, and he wants to set up all brouters to bridge. How would you make your recommendations address the IT director's interest in NetBEUI?
6. Also, after the upgrades have been completed and adjustments have been made to the campus workstations, the business office has discovered that four of their Windows 98 computers can no longer access their networked Hewlett Packard 4Si printers. What do you suggest?
7. The IT director is new because he was the Development Office's database manager who was recently promoted. He has heard about connectionless and connection-oriented services, but is not sure how these apply to protocols. Prepare an explanation of how they apply to TCP/IP and IPX/SPX.

Optional Case Projects for Teams

Team Case One

Mark Arnez has been hearing about the new version of IP, called IPv6 or IP Next Generation, which is under development. He asks that you form a team to research this developing protocol and to explain its advantages. How might the protocol affect the use of Windows 2000? Consider using the Internet to help in your research.

Team Case Two

Mark wants you to form a team to give a presentation about why TCP/IP has become the protocol of the Internet. Research the Internet — past, present, and future — and explain the full story of this relationship.